KU LEUVEN

FACULTEIT INGENIEURSWETENSCHAPPEN

Secure Messaging Service
Using A Bulletin Board

Benjamin Rübenkamp
R0793577
MEIsw
Master industrieel ingenieur Elektronica-ICT
Academiejaar 2023-2024

INHOUD

INLEIDING

Het ontwerp en de implementatie van het project belichten een veelzijdigheid aan doordachte beslissingen die zijn genomen om een veilig en schaalbaar gedistribueerd chatsysteem te creëren. Met de introductie van dynamische serverinstanties, asymmetrische cryptografie en multithreading wordt gestreefd naar een robuuste architectuur die de gebruikerservaring versterkt en gelijktijdig voldoet aan moderne veiligheidseisen. De dynamische aanpak van serverinstanties, waarbij het aantal servers zich aanpast naargelang de belasting, waarborgt een optimale inzet van resources. De implementatie van asymmetrische cryptografie, specifiek het Elliptic Curve Diffie-Hellman (ECDH) algoritme, biedt een solide basis voor het veilig uitwisselen van sleutels tussen clients. Het gebruik van multithreading maakt gelijktijdige interacties met meerdere clients mogelijk, waardoor de responsiviteit van het systeem toeneemt.

1.1 Dynamische Serverinstanties

Beslissing: Het systeem is ontworpen om dynamisch serverinstanties aan te maken of te verwijderen op basis van de belasting.

Motivering: Deze adaptieve aanpak zorgt voor efficiënt gebruik van resources. Nieuwe serverinstanties worden gestart wanneer de belasting toeneemt, en onderbenutte instanties worden verwijderd om het resourceverbruik te optimaliseren.

1.2 Asymmetrische cryptografie voor veilige communicatie

Beslissing: Asymmetrische cryptografie is geïmplementeerd met behulp van het Elliptic Curve Diffie-Hellman (ECDH)-algoritme om een veilig communicatiekanaal tussen klanten tot stand te brengen.

Motivering: Asymmetrische cryptografie zorgt voor een veilige sleuteluitwisseling tussen de client instanties, waardoor afluisteren wordt voorkomen.

1.3 Multithreading voor gelijktijdige klanten

Beslissing: Een multithreaded aanpak is geïmplementeerd om gelijktijdige uitvoering van meerdere klanten mogelijk te maken.

Motivering: Multithreading maakt parallelle verwerking van klantinteracties mogelijk, wat de responsiviteit verbetert. Elke klant draait in zijn eigen thread, waardoor onafhankelijke uitvoering wordt gegarandeerd en interferentie tussen klanten wordt vermeden.

2.1 Sterktes

Beveiligingsmaatregelen: Het project integreert versleutelings- en hash-technieken voor veilige communicatie, wat de gegevensprivacy en integriteit verbetert.

Gedistribueerde architectuur: Het gebruik van RMI en een load balancer maakt een schaalbaar en gedistribueerd systeem mogelijk, afgestemd op toenemende vraag.

Sleutelafleidingsfunctie: Implementatie van een KDF verhoogt de vertrouwelijkheid van communicatie door niet meerdere sleutels over het netwerk te hoeven verzenden.

2.2 Zwaktes

Foutafhandeling: Het project mist diepgaande foutafhandeling, wat kan leiden tot onverwacht gedrag in bepaalde scenario's. **Beperkte gebruikersinterface:** De grafische gebruikersinterface is minimaal en mist functies die de gebruikerservaring en interactie kunnen verbeteren.

Beperkte chatmogelijkheden: Chatten wordt alleen ondersteund met één persoon tegelijk. Er moet opnieuw worden gebumpt nadat één van de client instanties is afgesloten.

2.3 Kansen

Verbetering van de gebruikersinterface: Er is een kans om de gebruikersinterface te verbeteren door functies toe te voegen zoals real-time berichtupdates (zonder polling). Ook het aanbieden van chatten met meerdere mensen (groepschat en/of meerdere privéchats) en een intuïtiever ontwerp is een mogelijke uitbreiding.

Verbeterde foutafhandeling: Implementatie van robuustere foutafhandeling kan de betrouwbaarheid en beveiliging van het systeem verbeteren.

2.4 Bedreigingen

Naleving regelgeving: Veranderingen in regelgevende eisen met betrekking tot beveiliging kunnen uitdagingen opleveren.

Technologische veroudering: Snelle vooruitgang in technologie (bv kwantumcomputing) kan bepaalde cryptografische algoritmen of beveiligingsmaatregelen onbruikbaar maken, wat periodieke updates vereist.

BESLUIT

Dit project weerspiegelt een doordachte aanpak bij het ontwerpen van een gedistribueerd chatsysteem, waarbij strategische beslissingen zijn genomen om zowel schaalbaarheid als veiligheid te waarborgen.

De implementatie van dynamische serverinstanties biedt een flexibele oplossing voor het beheer van werkbelasting. De keuze voor asymmetrische cryptografie, versterkt de beveiliging van communicatie.

Het gebruik van multithreading draagt bij aan de responsiviteit van het systeem en de sterke nadruk op beveiligingsmaatregelen, zoals encryptie en hashing, draagt bij aan de bescherming van de privacy en integriteit van de gegevens.

Deze evaluatie, ondersteund door een SWOT-analyse, belicht de sterke punten van het project. Verder geeft het ook enkele beperkingen en mogelijke uitbreidingen. Tijdens de duur van dit project is veel bijgeleerd over beveiliging van data en RMI communicatie.